(12) UK Patent Application (19) GB (11) 2 329 096 (13) A

(43) Date of A Publication 10.03.1999

(21) Application No 9718200.0

(22) Date of Filing 29.08.1997

(51) INT CL[6]
H04L 9/32

(52) UK CL (Edition Q)
H4P PDCSP
U1S S2209

(56) Documents Cited
GB 2308282 A GB 2293737 A EP 0781003 A2
US 5608801 A

(58) Field of Search
UK CL (Edition P) H4P PDCSC PDCSL PDCSP
INT CL[6] G06F 12/14, H04L 9/32
Online:WPI,USPATFULL

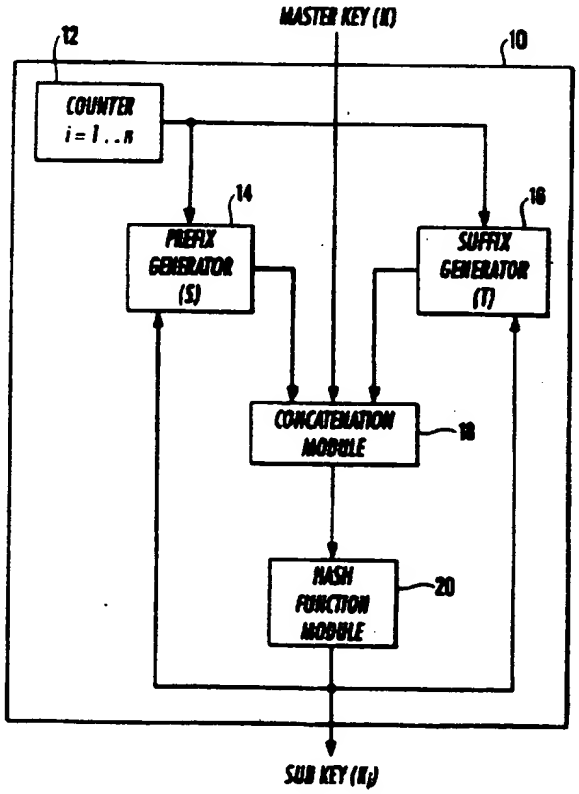
(71) Applicant(s)
Neipher Corporation Limited
(Incorporated in the United Kingdom)
Jupiter House, Station Road, Cambridge, CB1 2JD, United Kingdom

(72) Inventor(s)
Ian Nigel Harvey
Nicholas Benedict Van Someren

(74) Agent and/or Address for Service
Lewis & Taylor
144 New Walk, LEICESTER, LE1 7JA, United Kingdom

(54) Abstract Title
Creating sub-keys from hashed cryptographic master key

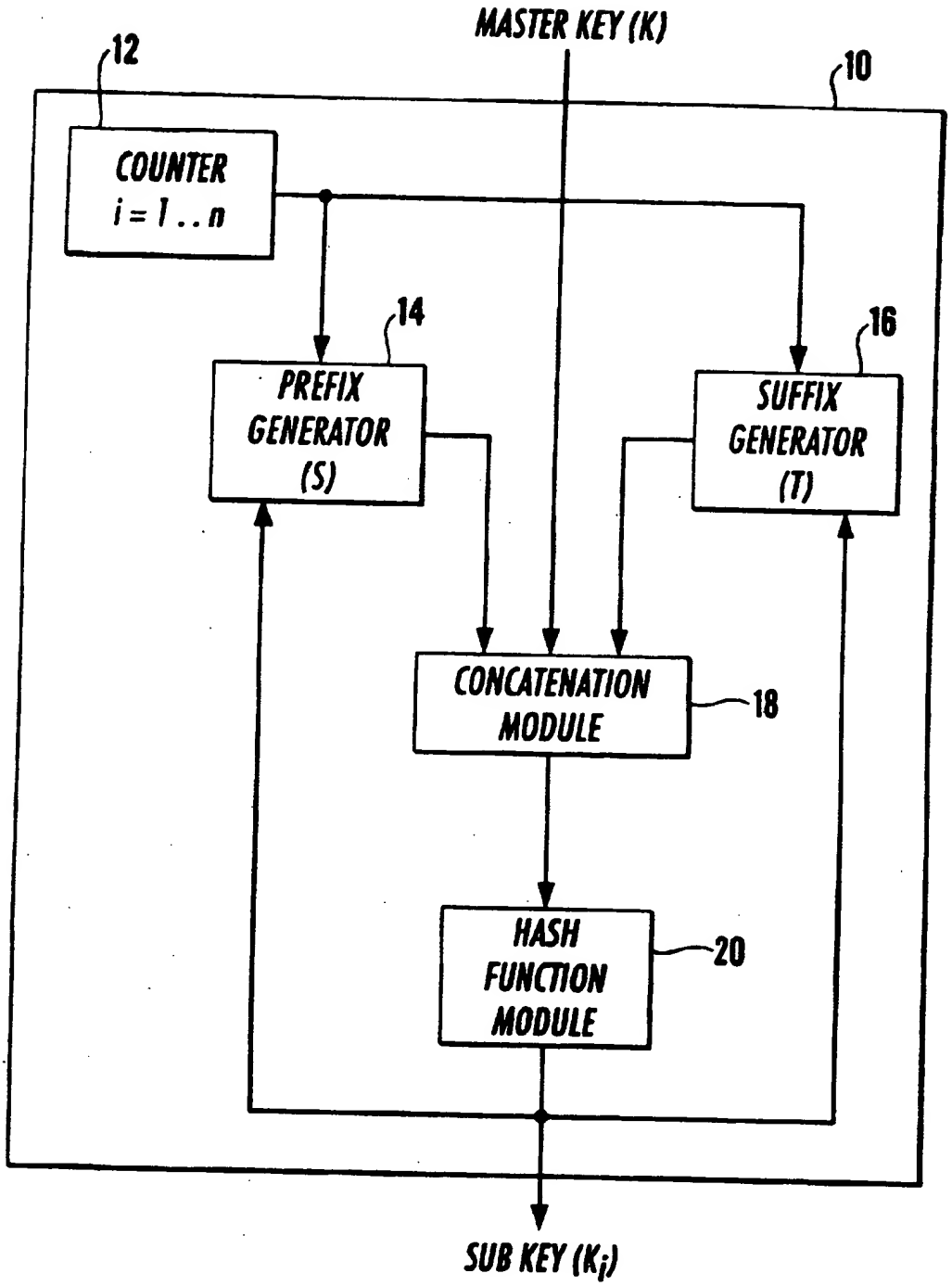
(57) A facility for enhancing data security comprises a plurality of encryption modules, an interface and a data processing machine (10). The encryption modules are each responsible to a sub-key for encrypting data. The interface is operative to receive a master key, and the data processing machine (10) is operative to create a series of sub-keys for use with the modules. The machine (10) is operative to create each of the sub-keys by means of a hash function of the master key.



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The print reflects an assignment of the application under the provisions of Section 30 of the Patents Act 1977.

GB 2 329 096 A


MASTER KEY (K)
12
10
COUNTER
i = 1 . . n
14
16
PREFIX
GENERATOR
(S)
SUFFIX
GENERATOR
(T)
CONCATENATION
MODULE
18
HASH
FUNCTION
MODULE
20
SUB KEY (Ki)

Title: Data Security

This invention is concerned with data security, and in particular to the security of data transferred in the course of commercial activities such as banking.

In the field of banking, data is transferred along data carriers in such a manner that a data stream can be intercepted by an unauthorised person. Hence, there is a need to disguise the data so that it can only be comprehended by the intended and authorised user.

In one method of disguising data, a cryptographic cipher system is used. If data is to be sent between a sender and a recipient along a channel which is of questionable security, then it is encrypted using a cipher implemented by the system.

Most ciphers require a secret "master key" to be shared between sender and recipient. In many systems, the master key is used by the cipher to generate a plurality of sub-keys which are used by internal functions of the cipher in the encryption process.

In the past, sub-keys have been derived either by re-ordering selected bits of the key data or by using a simple mathematical function such as an arithmetic progression.

The type of system described above is lacking in versatility, in that it expects a master key of a predetermined length, and cannot accommodate master keys of different lengths. It cannot deal with the generation of a variable number of sub-keys, which would improve security.

Furthermore, where there is a simple relationship between two master keys used with the above system, there may be a correspondingly simple relationship between the sets of sub-keys so produced. That relationship could easily be found by a cryptanalyst, and the security of a system protected in that manner could be compromised.

It is an object of the present invention to provide a system which ameliorates the above problems.

According to the invention there is provided a facility for enhancing data security, the facility comprising a plurality of encryption modules each being responsive to a sub-key for encrypting data, an interface for receiving a master key, and a data processing machine operative to create a series of sub-keys for use with the modules, the machine being operative to create each of the sub-keys by means of a hash function of the master key.

In that way, the series of sub-keys corresponding to a master key will not be evident to an unauthorised user.

Preferably, the hash function operates on a concatenation of the master key with at least one other piece of data. Therefore, the complexity of the result of the hash function is substantially increased which makes it more difficult for a pattern between the sub-keys and master key to be established.

The other data may comprise at least one of a constant, the position of the sub-key in the series, a function of the position of the sub-key in the series, preceding sub-keys in the series, and a function of preceding sub-keys in the series.

In a preferred embodiment of the invention, the concatenation comprises a first string of other data preceding the master key and a second string of other data following the master key, at least one of the first and second strings varies with the position in the series of the sub-key being calculated. In that way, the security of the cipher defined by the series of sub-keys is enhanced.

The hash function is preferably a one way hash function. In a preferred embodiment, the hash function is collision free.

In a preferred embodiment of the invention, the data processing machine derives the sub-keys of the series and then stores the series for later use by the sections.

Alternatively, the sub-keys are derived as they are required by the sections.

Preferably, the sub-keys are derived in the order in which they are to be used.

In a preferred embodiment of the invention, the hash function produces results the same length as the desired length of hash key. Alternatively, if the hash function results are shorter than the desired length of sub-key, then a sub-key can be constructed from a concatenation of hash function results. Furthermore, if the hash function results are longer than the desired length of sub-key, then more than one sub-key could be derived from a hash function result.

Further preferred aspects and features of the invention will be appreciated from the following description of a specific and preferred embodiment of the invention, with reference to the drawing appended hereto which shows a schematic diagram ilustrating the function of a data processing machine contained in a cryptographic system in accordance with the invention.

A cryptographic system comprises n sections, each acting on target data in response to a sub-key supplied to that section. Hence, the system as a whole is operated by a key schedule comprising a set of n sub-keys $\{K_1,K_2,...,K_n\}$.

The figure illustrates a sub-key data processing machine 10 having a series of interconnected modules.

A counter 12 generates a counter signal having value between 1 and n, where n is the number of sections of the system and thus the number of sub-keys to be generated.

A prefix generator 14 and a suffix generator 16 are provided, the generators 14, 16 being operative to generate values S_i and T_i respectively.

S_i, T_i, and a master key K are fed forward to a concatenation module 18 where the data is concatenated, and then the concatenated data is fed to a hash function module 20

A key schedule is derived from the master key K, by means of a hash function embodied in the hash function module 20 as follows:

$$K_i = H(S_i \mid K \mid T_i) \qquad 1 \le i \le n,$$

where $H()$ is a hash function, the | symbol represents concatenation of data and S_i and T_i are generated in the prefix and suffix generators 14, 16 as indicated above. S_i and T_i may be constructed from some or any of:

(1) a constant value;

(2) the value i;

(3) a function of the value i;

(4) any of the values $K_1,\ldots,K_{i-1}$;

(5) a function of the values $K_1,\ldots,K_{i-1}$.

The sub-keys are used in order, so that the first use of K_i is after the first use of each of $K_1,\ldots,K_{i-1}$. This is an optional arrangement which allows sequential production of sub-keys, such as in the case where a sub-key is a function of preceding sub-keys. As shown in the drawing, the result output by the hash function module 20 is fed back to the prefix and suffix generators 14, 16 so that they can utilise the result in later iterations. The machine can thus derive each sub-key as it is needed. However, it may be more useful for the machine to derive all of the sub-keys at an initial stage and store them in turn for later use.

In some cases, the length of the sub-keys required for the sections of the system is less than the length of the output of the hash function. In that case, the result of each hash operation can be used to make more than one sub-key. If the length of the sub-key required is greater than the length of the output of the hash function, the outputs of several hash operations can be concatenated to construct the sub-key.

In order to ensure that the key schedule is "strong", i.e. that it is not susceptible to deciphering, at least one of S_i and T_i varies with the value of i.

For optimal security, the hash function $H()$ should be chosen to be one way and collision free.

The system described above is useful in that it is capable of defining a master key of arbitrary length. Moreover, a variable number of sub-keys of variable length can be generated from each master key. The system avoids "weak" keys from which a pattern can be derived easily, and is generally more robust against cryptanalysis than previous encryption systems, since there is no simple relationship between sub-keys generated from master keys which have a simple relationship.

CLAIMS

1. A facility for enhancing data security, the facility comprising a plurality of encryption modules each being responsive to a sub-key for encrypting data, an interface for receiving a master key, and a data processing machine operative to create a series of sub-keys for use with the modules, the machine being operative to create each of the sub-keys by means of a hash function of the master key.

2. A facility in accordance with claim 1 wherein the hash function operates on a concatenation of the master key with at least one other piece of data.

3. A facility in accordance with claim 2 wherein the other place of data comprises at least one of a constant, the position of the sub-key in the series, a function of the position of the sub-key in the series, preceding sub-keys in the series, and a function of preceding sub-keys in the series.

4. A facility in accordance with claim 2 or claim 3 wherein the concatenation comprises a first string of other data preceding the master key and a second string of other data following the master key, at least one of the first and second strings varies with the position in the series of the sub-key being calculated.

5. A facility in accordance with any preceding claim wherein the hash function is a one way hash function.

6. A facility in accordance with claim 5 wherein the hash function is collision free.

7. A facility in accordance with any preceding claim wherein the data processing machine derives the sub-keys of the series and then stores the series for later use by the sections.

8. A facility in accordance with any one of claims 1 to 6 wherein the sub-keys are derived as they are required by the sections.

9. A facility in accordance with claim 7 or claim 8 wherein the sub-keys are derived in the order in which they are to be used.

10. A facility in accordance with any preceding claim the hash function produces results the same length as the desired length of sub-key.

11. A facility of enhancing data securing as described with reference to the accompanying drawing.

The Patent Office

8

Application No:	GB 9718200.0	**Examiner:**	B.J.SPEAR
Claims searched:	1-11	**Date of search:**	14 January 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PDCSC, PDCSP, PDCSL)

Int Cl (Ed.6): G06F 12/14, H04L 9/32

Other: Online:WPI, USPATFULL

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
XY	GB2308282A	(Lotus) Whole document, eg Figs. 1, !A; page 8 line 8 to page 9 line 19 ; claims 1,8. Published 18/6/97.	1,2,5,6 at least
A	GB2293737A	(Pitney Bowes). See definition of hash on page 5 lines 10-19.	
Y	EP0781003A2	(General Instrument) Whole document, eg claim 1. Published 25/6/97	1 at least
X	US5608801	(Bell) Whole document, eg claim 1.	1,2 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.